NRI 未来創発
Dream up the future.

NRIセキュアテクノロジーズ
NRI SecureTechnologies

News Release

2015 年 7 月 30 日
NRI セキュアテクノロジーズ株式会社

「セキュリティログ監視サービス フォレンジック パッケージ」を米国で提供開始

～ソリトン社の EDR 技術と自社のセキュリティ管理サービスを融合～

NRI セキュアテクノロジーズ株式会社（本社：東京都千代田区、代表取締役社長：小田島 潤、以下「NRI セキュア」）は、自社システムがコンピュータウイルスに感染するといったセキュリティインシデント（事案）の発生時に、原因分析と対応（フォレンジック[*1]）を迅速におこなえる「セキュリティログ監視サービス フォレンジックパッケージ」（以下「本サービス」）を、9 月 4 日から米国で提供開始します。

本サービスにおいては、ソリトン社[*2]の持つ EDR 技術[*3] と NRI セキュアの提供する監視サービス[*4]を融合することにより、本社から離れた拠点で生じたセキュリティインシデントであっても、速やかに的確な対処が可能となります。

マルウェア[*5]への感染等、セキュリティインシデントの発生が疑われた場合、問題となる端末の隔離と調査、および他の端末への二次被害状況の確認が必要となります。この一連の作業には、フォレンジック技術が有効ですが、自社でその技術を持つ専門性の高い人材を確保することは困難です。さらにインシデントが遠隔地で発生した場合、現地への調査員の派遣、もしくは当該端末の調査部門への輸送に時間を有します。二次感染や情報漏えいなどの被害が拡大してしまう可能性も考えられ、特に世界中に多くの拠点を持つ企業にとって、深刻な問題となっています。

このような課題を解決するため、NRI セキュアは本サービスを開発しました。主な機能と特長は、以下のとおりです。

■ソリトン社の EDR 技術を利用して端末情報を常時収集

EDR エージェント[*6]を企業内の端末にインストールし、端末の操作履歴やネットワーク接続、レジストリ[*7]更新、ファイル遷移、プロセスなどの詳細ログ情報を、平常時から収集します。

■セキュリティログ監視サービスを 24 時間 365 日提供

NRI セキュアの専門スタッフが、24 時間 365 日でログ情報を収集しつつ、セキュリティ攻撃の有無を遠隔地から監視します。収集するログ情報には、上記の EDR エージェントから収集した情報も含みます。

■ログを常時事前取得することにより、迅速なフォレンジックが可能

セキュリティログ監視サービスによって、マルウェア感染の疑いがある端末が発見されると、その端末内で生じたデータの移動やコピーなどの動作情報を、本サービスを導入した企業と共有し、そのデータが機密情報に該当するか、情報漏えいが生じているか、などを明らかにします。さらに、該当端末の感染原因を特定し、再発防止策を導入企業へ提案すると同時に、取得したマルウェアの特性情報を元に、企業内の他の端末への二次感染の有無を迅速に把握し、被害の拡大防止をおこないます。これら一連の作業（フォレンジック）に必要な端末情報は、EDR エージェントからすでに収集済みのログ情報を用いて実施するため、インシデントが発生してから専門家が情報収集をおこなう従来型の作業と比較して、大幅に対応までの時間を短縮できます。

このサービスは、現在 NRI セキュアが提供中の、セキュリティログ監視サービスの機能強化版として、まずは遠隔地でのフォレンジック需要の高い米国で提供を開始します。今後、日本や他の地域でのサービス提供も予定しており、グローバル企業の情報セキュリティ対策を支援します。

NRI セキュアは、今後も、グローバル企業の情報セキュリティ対策を支援するさまざまなサービスを提供し、安全・安心な情報システム環境と社会の実現に貢献していきます。

*1 フォレンジック：セキュリティ事故が起きた際に、端末やネットワーク内の情報を収集し、被害状況の解明や犯罪捜査に必要な法的証拠を明らかにする取り組み。「鑑識」「科学捜査」の意味でも使われる

*2 ソリトン社：株式会社ソリトンシステムズ（本社：東京都新宿区、代表取締役社長：鎌田信夫）。サイバー攻撃対策や認証・アクセス制御ソリューションを始めとする IT セキュリティ製品の開発とサービスを提供する独立系ベンダー

*3 EDR（Endpoint Detection and Response）技術：エンドポイント（端末）監視技術。OS に標準的に搭載されているログ取得機能と比較して、より広範囲に、より詳細なログ取得を実現できる特徴がある

*4 監視サービス（セキュリティログ監視サービス）： NRI セキュアが 2014 年 11 月 19 日に発表した、企業の情報システムで利用されているさまざまな機器（サーバ、ネットワーク機器、クライアント端末など）が出力するアクセス履歴等のログ情報を、独自の技術で分析し、迅速にセキュリティインシデントを見つけ出すサービス。詳細は、http://www.nri-secure.co.jp/news/2014/1119.html を参照

*5 マルウェア：コンピュータウイルスやワームなど、悪意のある不正なソフトウエアの総称

*6 EDR エージェント：端末上の動作をログとして詳細に記録し、そのログを保管のために外部サーバへ転送するプログラム

*7 レジストリ：OS やソフトなどの各種設定が保管されているデータベース

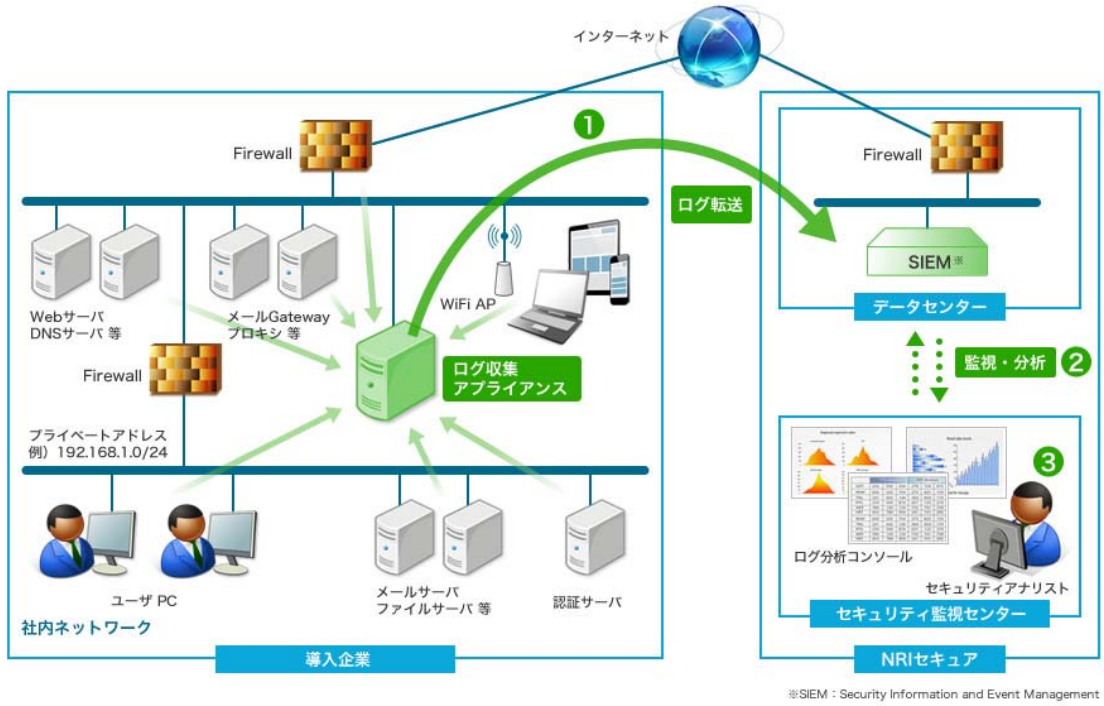
【ニュースリリースに関するお問い合わせ】
株式会社野村総合研究所　コーポレートコミュニケーション部　潘、十河
TEL：03-6270-8100　E-mail：kouhou@nri.co.jp

【サービスに関するお問い合わせ】

NRI セキュアテクノロジーズ株式会社　北米支社　松下
TEL：+1-949-537-2957（米国）　E-mail：info@nri-secure.co.jp
NRI セキュアテクノロジーズ株式会社　広報担当　根本
TEL：03-6706-0622　E-mail：info@nri-secure.co.jp

【ご参考】

■サービス概要図



① 導入企業内に設置したログ収集アプライアンス（装置）が、EDR エージェントをインストールした PC 端末、およびその他の情報システム機器から出力されるログを自動的に収集し、NRI セキュアデータセンター内の SIEM（セキュリティ情報イベント管理の仕組み）に転送します。

② NRI セキュアのデータセンターで、転送されたログに対して、NRI セキュアが独自に設計したロジックによる相関分析をおこないます。

③ セキュリティ監視センターで、セキュリティアナリストが 24 時間 365 日の体制で監視・分析をおこない、セキュリティインシデントを迅速に発見し、必要に応じて EDR エージェントのログとソリトン社のデータ分析の経験を活用することで、端末へのフォレンジックを実施します。

*SIEM（Security Information and Event Management/セキュリティ情報イベント管理）：サーバやネットワーク機器などの各種アプリケーションから集められたログ情報を一元的に蓄積・管理し、異常があった場合いち早く検知・分析をする仕組み